



Billing Code: 3510-BX

DEPARTMENT OF COMMERCE

[Docket No.: 170502443-7443-01]

Privacy Act of 1974; System of Records

AGENCY: U.S. Department of Commerce, Office of the Secretary.

ACTION: Notice of Proposed Amendment to Privacy Act System of Records:

COMMERCE/DEPT-13, Investigative and Security Records.

SUMMARY: In accordance with the Privacy Act of 1974, as amended, The Freedom of Information Act, as amended; and Office of Management and Budget (OMB) Circular A-108, “Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act,” the Department of Commerce (Department) is issuing a notice of intent to establish an amended system of records entitled, COMMERCE/DEPT-13, “Investigative and Security Records.” This action is necessary to update the types or categories of information maintained, and update dated information covered by the current COMMERCE/DEPT-13 system of records notice. We invite public comment on the system amended announced in this publication.

DATES: To be considered, written comments must be submitted on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. The Department filed a report describing the modified system of records covered by this notice with the Chair of the Senate Committee on Homeland Security and Governmental Affairs, the Chair of the House Committee on Oversight and Government Reform, and the Deputy Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget (OMB), on May 31, 2017. This modified system of records will become effective upon publication in the FEDERAL REGISTER on [INSERT DATE OF PUBLICATION IN THE FEDERAL

REGISTER], unless the modified system of records notice needs to be changed as a result of public comment.

Newly proposed routine uses 11, 12, 13, and 14 in the paragraph entitled “ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES” will become effective on [INSERT DATE 45 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], unless the modified system of records notice needs to be changed as a result of public comment. If the modified system of records notice needs to be changed, the Department will publish a subsequent notice in the FEDERAL REGISTER by [INSERT DATE 45 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], stating that the current system of records will remain in effect until a revised notice is published in the FEDERAL REGISTER.

ADDRESSES: You may submit written comments by any of the following methods:

Email: mtoland@doc.gov. Include “COMMERCE/DEPT-13, Investigative and Security Records” in the subject and subtext of the message.

Mail: Michael J. Toland, Ph.D., Deputy Chief Freedom of Information Act Officer and Department Privacy Act Officer, Office of Privacy and Open Government, 1401 Constitution Ave. NW., Room 52010, Washington, DC 20230.

FOR FURTHER INFORMATION CONTACT: Michael J. Toland, Ph.D., Deputy Chief Freedom of Information Act Officer and Department Privacy Act Officer, Office of Privacy and Open Government, 1401 Constitution Ave. NW., Room 52010, Washington, DC 20230.

SUPPLEMENTARY INFORMATION: The Office of Security IT Infrastructure allows the Department’s Office of Security (OSY) the ability to fulfill its responsibility for investigative and security records by providing OSY personnel with the tools (hardware, software, and

training) and access to the internal and external information resource necessary to perform their responsibilities. The system controls access to only those authorized as well as aids in the monitoring, assessment and response to security and emergency related incidents.

SYSTEM NAME AND NUMBER: Investigative and Security Records,
COMMERCE/DEPT-13.

SECURITY CLASSIFICATION: Sensitive but unclassified.

SYSTEM LOCATION: U.S. Department of Commerce Office of Security HCHB Consolidated Server Room (CSR), 1401 Constitution Ave. NW, Washington, DC 20230.

SYSTEM MANAGER(S): Director, Office of Security, Herbert C. Hoover Building,
Washington, DC 20230.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; Equal Employment Act of 1972; and all existing, applicable Department policies, and regulations.

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to collect and maintain records of processing of personnel security-related clearance actions, to record suitability determinations, to record whether security clearances are issued or denied, and to verify eligibility for access to classified information or assignment to a sensitive position. Also, records may be used by the Department for adverse personnel actions such as removal from sensitive duties, removal from employment, denial to a restricted or sensitive area, and/or revocation of security clearance. The system also assists in capturing background investigations and adjudications; directing the clearance process for granting, suspending, revoking and denying access to classified information; directing the clearance process for granting, suspending,

revoking and denying other federal, state, local, or foreign law enforcement officers the authority to enforce federal laws on behalf of the Department; managing state, local and private-sector clearance programs and contractor suitability programs; determining eligibility for unescorted access to Department owned, occupied or secured facilities or information technology systems; and/or other activities relating to personnel security management responsibilities at the Department.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Categories of individuals covered by this system include past and present federal employees, applicants, contractors, affiliates who require: (1) access to Department-owned or operated facilities, including commercial facilities operating on behalf of the Department; (2) access to Department information technology (IT) systems and data; or (3) access to national security information including classified information.

CATEGORIES OF RECORDS IN THE SYSTEM: The records in the system contain social security number; passport number; name; maiden name; alias; gender; race/ethnicity; date of birth; place of birth; home address; telephone number; email address; education; financial information; medical information; military service; physical characteristics; mother's maiden name; citizenship, former residency; employment; people who know you; marital status; relatives; foreign contacts, foreign activities; foreign business; foreign travel; police record; investigations and clearance information; use of information technology; involvement in non-criminal court actions and associations; job title; work address; telephone number; email address; work history; employment history; fingerprints; scars, marks, tattoos; eye color; hair color; height; and weight. This system does not include records of Equal Employment Opportunity (EEO) investigations. Such records are covered in a government-wide system notice by the

Office of Personnel Management and are now the responsibility of the Equal Employment Opportunity Commission. For assistance contact the Department Privacy Act Officer, Office of Privacy and Open Government, 1401 Constitution Ave. NW, Room 52010, Washington, DC 20230.

RECORD SOURCE CATEGORIES: Subject individuals; OPM, FBI and other Federal, state and local agencies; individuals and organizations that have pertinent knowledge about the subject; and, those authorized by the individual to furnish information.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

1. In the event that a system of records maintained by the Department to carry out its functions indicates a violation or potential violation of law or contract, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute or contract, or rule, regulation, or order issued pursuant thereto, or the necessity to protect an interest of the Department, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether federal, state, local or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute or contract, or rule, regulation or order issued pursuant thereto, or protecting the interest of the Department.
2. A record from this system of records may be disclosed, as a routine use, to a federal, state or local agency maintaining civil, criminal or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a Department decision concerning the assignment, hiring or retention of an

individual, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant or other benefit.

3. A record from this system of records may be disclosed, as a routine use, to a federal, state, local, or international agency, in response to its request, in connection with the assignment, hiring or retention of an individual, the issuance of a security clearance, the reporting of an investigation of an individual, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.
4. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
5. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual when the individual has requested assistance from the Member with respect to the subject matter of the record.
6. A record in this system of records may be disclosed, as a routine use, to the Department of Justice in connection with determining whether disclosure thereof is required by the Freedom of Information Act (5 U.S.C. 552).
7. A record in this system of records may be disclosed, as a routine use, to a contractor of the Department having need for the information in the performance of the contract, but not operating a system of records within the meaning of 5 U.S.C. 552a(m).
8. A record in this system of records may be disclosed, as a routine use, to the National Archives and Records Administration or other federal government agencies pursuant to

records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

9. A record in this system of records may be disclosed, as a routine use, to an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.
10. A record in this system of records may be disclosed to appropriate agencies, entities and persons when: (1) it is suspected or determined that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and to prevent, minimize, or remedy such harm.
11. A record in this system of records may be disclosed to another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

12. A record in this system of records may be disclosed to an individual's prospective or current employer to the extent necessary to determine employment eligibility.
13. A record in this system of records may be disclosed to third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate to the proper performance of the official duties of the officer making the disclosure.
14. A record in this system of records may be disclosed to a public or professional licensing organization when such information indicates, either by itself or in combination with other information, a violation or potential violation of professional standards, or reflects on the moral, educational, or professional qualifications of an individual who is licensed or who is seeking to become licensed.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records are stored on servers, magnetic disc, tape, digital media, and CD-ROM.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may generally be retrieved by individual's name, date of birth, social security number, if applicable, or other unique individual identifier.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

When cases are closed, records are disposed of in accordance with General Records Schedule 3 – Procurement, Supply, and Grant Records; General Records Schedule 9 – Travel and Transportation Records; and General Records Schedule 18 – Security and Protective Services Records.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable Department automated systems security and access policies. Strict controls have been imposed to minimize risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties, who have appropriate clearances or permissions, and who have taken Privacy Act training.

RECORD ACCESS PROCEDURES:

An individual requesting access to records on himself or herself should send a signed, written inquiry to the same address as stated in the Notification Procedure section above. The request letter should be clearly marked, "PRIVACY ACT REQUEST." The written inquiry must be signed and notarized or submitted with certification of identity under penalty of perjury.

Requesters should specify the record contents being sought.

CONTESTING RECORD PROCEDURES:

An individual requesting corrections or contesting information contained in his or her records must send a signed, written request inquiry to the same address as stated in the Notification Procedure section below. Requesters should reasonably identify the records, specify the information they are contesting and state the corrective action sought and the reasons for the correction with supporting justification showing how the record is incomplete, untimely, inaccurate, or irrelevant. The Department's rules for access, for contesting contents, and for appealing initial determination by the individual concerned appear in 15 CFR part 4, Appendix B.

NOTIFICATION PROCEDURE:

An individual requesting notification of existence of records on himself or herself should send a signed, written inquiry to the Deputy Chief FOIA Officer and Department Privacy Act Officer, Room 52010, U.S. Department of Commerce, 1401 Constitution Avenue NW., Washington, DC 20230.

For more information, visit:

http://www.osec.doc.gov/opog/PrivacyAct/PrivacyAct_requests.html.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: Pursuant to 5 U.S.C. 552a (k)(1), (k)(2) and (k)(5), all information and material in the record which meets the criteria of these subsections are exempted from the notice, access, and contest requirements under 5 U.S.C. 552a (c)(3), (d), (e)(1), (e)(4) (G), (H), and (I), and (f) of the agency regulations because of the necessity to exempt this information and material in order to accomplish the law enforcement function of the agency, to prevent disclosure of classified information as required by Executive Order 12065, to assure the protection of the President, to prevent subjects of investigation from frustrating the investigatory process, to prevent the disclosure of investigative techniques, to fulfill commitments made to protect the confidentiality of information, and to avoid endangering these sources and law enforcement personnel.

HISTORY:

<https://www.gpo.gov/fdsys/pkg/PAI-2013-COMMERCE/xml/PAI-2013-COMMERCE.xml#dept13>.

Dated: February 6, 2018.

Michael J. Toland,
Department of Commerce,
Deputy Chief FOIA Officer,
Department Privacy Act Officer.
[FR Doc. 2018-02687 Filed: 2/9/2018 8:45 am; Publication Date: 2/12/2018]